RISK ASSESSMENT PADA MANAJEMEN RESIKO KEAMANAN INFORMASI MENGACU PADA *BRITISH STANDARD ISO/IEC* 27005 *RISK MANAGEMENT*

Fajar Ilham Satria Yudha[1], Rd. Erwin Gunadhi[2]

Jurnal Algoritma
Sekolah Tinggi Teknologi Garut
Jl. Mayor Syamsu No. 1 Jayaraga Garut 44151 Indonesia
Email : jurnal@sttgarut.ac.id

[1]1206043@sttgarut.ac.id
[2]erwin.gunadhi@sttgarut.ac.id

Abstrak – *Badan Pertanahan Nasional (BPN) adalah Lembaga Pemerintah Non Kementrian yang berada di bawah dan bertanggung jawab kepada Presiden dan dipimpin oleh Kepala. (Sesuai dengan Perpres No. 63 Tahun 2013). Badan Pertanahan Nasional mempunyai tugas melaksanakan tugas pemerintahan di bidang pertanahan secara nasional, regional dan sektoral sesuai dengan ketentuan peraturan perundang-undangan.. Tujuan dari penelitian ini yaitu dapat mengetahui kondisi keamanan dan memberikan hasil dari Risk Assessment berdasarkan assessment yang mengikuti panduan standar ISO dalam hal mengidentifikasi resiko, kontrol, kelemahan dan lain – lain. Di mulai dari proses awal assessment sampai evaluasi. Metode yang di gunakan adalah Risk Assessment standar ISO/IEC 27005:Risk Management yang di dalamnya menerangkan tahapan – tahapan tentang Risk Assessment di antaranya Risk Identification, Risk Estimation dan Risk Evaluation. Hasil dari penelitian ini yaitu di dapatkannya hasil akhir berupa ranking akhir setiap resiko yang telah di beri penilaian dan di urutkan berdasarkan proses assessment menurut panduan BS ISO/IEC 27005.*

Kata Kunci – *Risk Assessment, ISO 27005, BPN (Badan Pertanahan Nasional), CIA (Confidentiality, Integrity, Availability), Sistem Manajemen Keamanan Informasi.*

I. PENDAHULUAN

Konsep kerahasiaan, keutuhan, dan ketersediaan (*Confidentiality, integrity & availability*) adalah hal pokok yang paling diperhatikan dalam menjaga faktor – faktor keamanan sistem suatu informasi karena dengan tidak terjaganya salah satu faktor tadi akan menjadi gerbang terbukanya masalah – masalah lain dalam keutuhan informasi yang tidak terjamin keamanannya. Badan Pertanahan Nasional dapat di kategorikan sebagai intansi negara yang bersifat memberikan pelayanan kepada publik, standar ISO/SNI telah memberikan panduan bagaimana untuk menerapkan keamanan sistem yang terstruktur dan jika memenuhi penilaian yang terukur dalam acuan standar ISO, maka organisasi ini akan di beri sertifikasi ISO/IEC 27001 oleh badan sertifikasi tertentu yang sudah terakreditasi. Objek penelitian pada Assessment yaitu sebuah infrastruktur aliran data digital data – data pertanahan dan database OLTP serta OLAP. Ada beberapa penelitian yang telah di lakukan tentang penerapan standar keamanan sistem seperti misalnya oleh Lisaura Dwi Kusuma, Patdono Suwignjo, dan Syarifa Hanoum. dengan judul "Risk Assessment pada Proyek Packing Plant Semen Gresik (PERSERO) TBK Menggunakan Framework ISO 31000 dan Metode Value at Risk".

II. TINJAUAN PUSTAKA

A. Keamanan Informasi

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan (Budi : 2005).

Keamanan informasi merupakan kegiatan penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimalisir resiko bisnis dan memaksimalkan peluang bisnis (ISO 27001 dalam Sarno dan Iffano, 2009: 27). Pengelolaan terhadap keamanan dapat dilihat dari sisi pengelolaan resiko (risk management). Lawrie Brown dalam menyarankan menggunakan "*Risk Management Model*" untuk menghadapi ancaman (managing threats). Ada tiga komponen yang memberikan kontribusi kepada *Risk*, yaitu *Asset*, *Vulnerabilities*, dan *Threats*

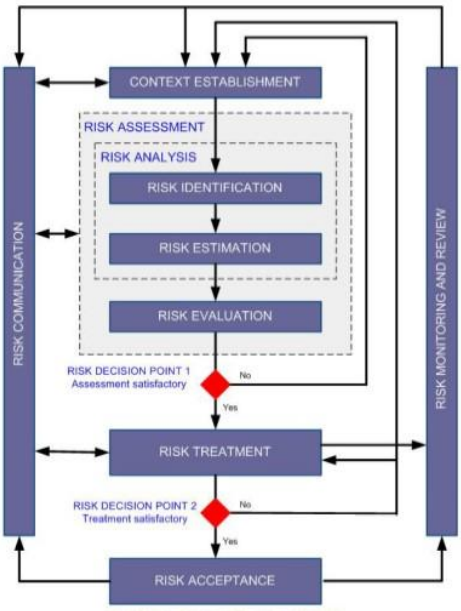
Untuk menanggulangi resiko (*Risk*) tersebut dilakukan apa yang disebut "*countermeasures*" yang dapat berupa :

- usaha untuk mengurangi *Threat*
- usaha untuk mengurangi *Vulnerability*
- usaha untuk mengurangi impak (*impac*t)
- mendeteksi kejadian yang tidak bersahabat (*hostile event*)
- kembali (*recover*) dari kejadian (Budi : 2005)

B. Manajemen Resiko Keamanan Informasi (*Information Security Risk Management*)

Pada panduan ISO/IEC 27005:*Information Security Risk Management*, Manajemen Resiko Keamanan Informasi terdiri dari beberapa tahap diantaranya *Establishing Context* lalu *Risk Assessment*, *Risk Treatment* dan *Risk Acceptance*.

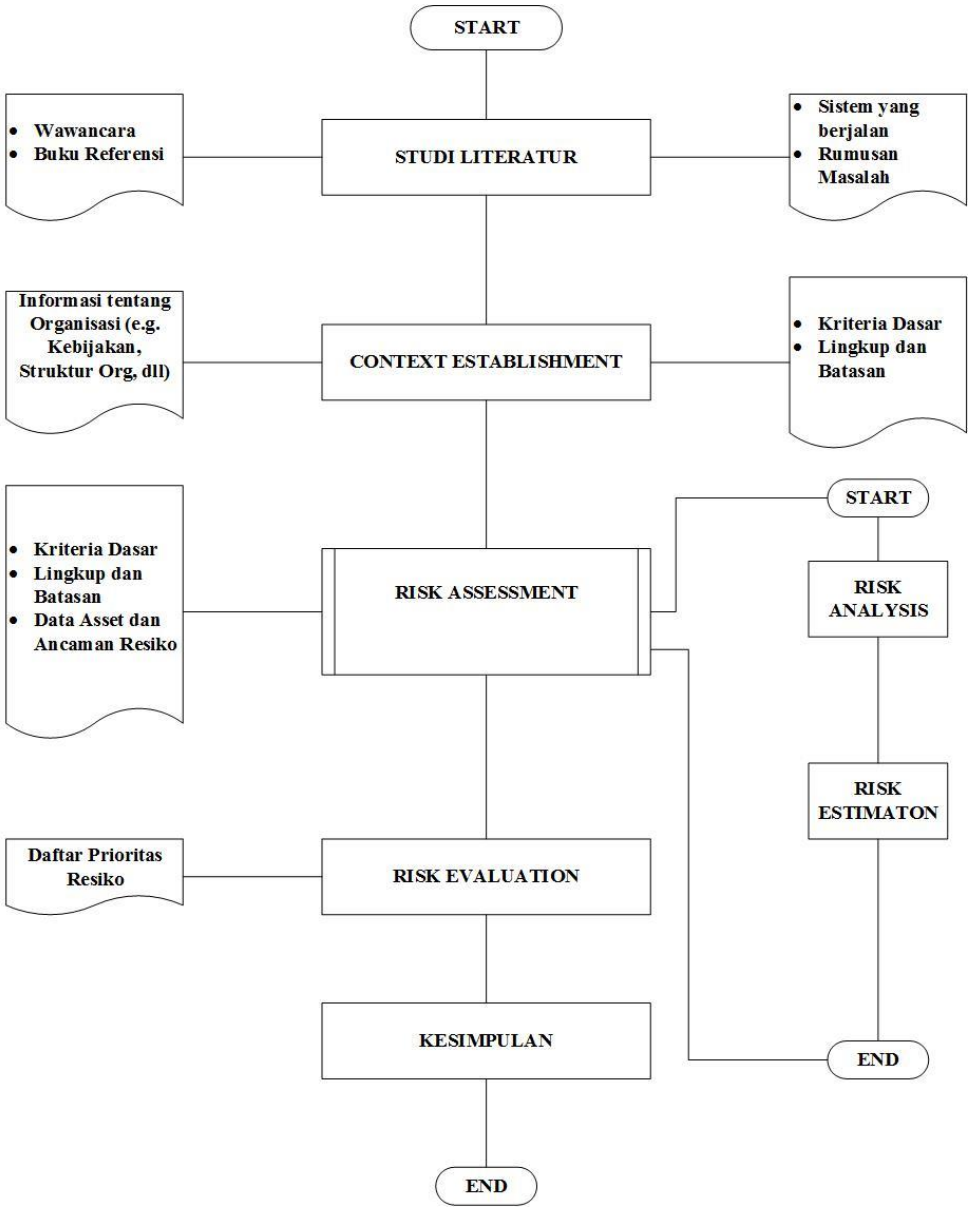
Risk Management dapat menganalisis apa yang akan terjadi dan konsekuensi apa yang akan di dapat, sebelum memutuskan apa yang harus di lakukan dan kapan untuk mengurangi resiko ke level yang dapat di terima (*Acceptable*)



III. KERANGKA KERJA KONSEPTUAL

A. Skema Kerja Penelitian

Tahapan aktivitas penelitian ini dijelaskan oleh kerangka kerja penelitian pada gambar 3.1.



Gambar 3.1 Kerangka Kerja Penelitian

IV. HASIL DAN PEMBAHASAN

A. Analisis Resiko

Tahapan awal Analisis Resiko yaitu yang terdiri dari identifikasi Aset dan identifikasi ancaman dan konsekuensi yang akan di jelaskan pada sub-bab berikut.

Identifikasi Aset

Setelah melakukan kajian pustaka berikut *Asset* yang telah berhasil teridentifikasi secara global teridentifikasi:

Tabel** Error! No text of specified style in document..**1 Daftar Asset Teridentifikasi

Asset ID	***Asset Name***
A1	Berkas Dokumen Sertifikat Pertanahan dan Peta Pertanahan
A2	Data Digital Dokumen Sertifikat Pertanahan dan Peta Pertanahan
A3	Program Larasita
A4	Database OLTP BPN, Warehouse Database OLAP, dan Database Konsolidasi
A5	Hardware
A6	Software
A7	Lingkungan Situs
A8	Jaringan
A9	Pegawai
A10	Organisasi

B. Evaluasi Resiko (*Risk Evaluation*)

Langkah pertama untuk evaluasi disini yaitu dengan membuat tabel yang berisi input data Asset yang terkena dampak, lalu memasukan nilai resikonya dan nilai dampak. tingkat resiko di ambil dari Threat Measure x Impact Value. Setelah itu resiko dapat di susun berdasarkan ranking dan di prioritaskan.

Tabel** Error! No text of specified style in document..**2 Menghitung Tingkat Resiko dan Prioritas Resiko

Asset ID	Threat ID	Threat Measure	Impact Value	Measure of Risk	Risk Ranking
A1	T1	**7**	**4**	**28**	**2**
	T2	**5**	**4**	**20**	**5**
	T3	**5**	**2**	**10**	**10**
	T4	**4**	**5**	**20**	**5**
A2	T1	**4**	**3**	**12**	**9**
	T2	**4**	**3**	**12**	**9**
	T3	**6**	**3**	**18**	**6**
A3	T1	**7**	**3**	**21**	**4**
	T2	**7**	**3**	**21**	**4**
	T3	**5**	**4**	**20**	**5**
A4	T1	**5**	**2**	**10**	**10**
	T2	**4**	**4**	**16**	**7**
	T3	**8**	**4**	**32**	**1**
	T4	**6**	**3**	**18**	**6**
	T5	**5**	**3**	**15**	**8**
A5	T1	**4**	**4**	**16**	**7**
	T2	**4**	**3**	**12**	**9**
	T3	**4**	**3**	**12**	**9**

	T4	**5**	**2**	**10**	**10**
	T5	**7**	**4**	**28**	**2**
A6	T1	**6**	**3**	**18**	**6**
	T2	**5**	**3**	**15**	**8**
	T3	**6**	**3**	**18**	**6**
	T4	**4**	**4**	**16**	**7**
	T5	**5**	**3**	**15**	**8**
	T6	**5**	**2**	**10**	**10**
A7	T1	**4**	**2**	**8**	**11**
	T2	**2**	**4**	**8**	**11**
A8	T1	**4**	**2**	**8**	**11**
	T2	**5**	**3**	**15**	**8**
	T3	**5**	**4**	**20**	**5**
	T4	**4**	**2**	**8**	**11**
	T5	**6**	**2**	**12**	**9**
	T6	**5**	**2**	**10**	**10**
	T7	**5**	**3**	**15**	**8**
A9	T1	**5**	**3**	**15**	**8**
	T2	**6**	**3**	**18**	**6**
	T3	**5**	**3**	**15**	**8**
	T4	**6**	**4**	**24**	**3**
	T5	**3**	**4**	**12**	**9**
	T6	**3**	**2**	**6**	**12**
	T7	**3**	**2**	**6**	**12**
A10	T1	**3**	**2**	**6**	**12**
	T2	**3**	**2**	**6**	**12**
	T3	**3**	**2**	**6**	**12**
	T4	**3**	**2**	**6**	**12**
	T5	**3**	**2**	**6**	**12**
	T6	**3**	**2**	**6**	**12**

Berikut urutan ranking resikonya, resiko di beri ranking berdasarkan tingkat resikonya dimulai dari yang tertinggi sampai resiko terendah.

Tabel** Error! No text of specified style in document.**.3** **Risk Ranking and Description

RISK RANK	*ASSET ID*	*THREAT ID*	*DESCRIPTION*
1	A4	T3	Asset terkena Virus pada asset utama yang paling penting menyebabkan kerusakan data, dan sistem
2	A1	T1	Keruskan berkas asset data pertanahan secara fisik maupun digital
2	A5	T5	Kerusakan alat penyimpaan hardware dokumen karena debu dan korosi

3	A9	T4	Kesadaran keamanan kurang dari pegawai sehingga keamanan asset data memiliki banyak celah kelemahan (*High Chance*)
4	A3	T1	Perenggangan waktu menyebabkan penyelesaian yang tidak efisien
		T2	Kesulitan dalam menangani pendaftar yang sangat banyak
5	A1	T2	Ada kesempatan kehilangan data namun jarang terjadi
		T4	Kerusakan data karena bencana alam memiliki likelihood minim namun tetap
	A3	T3	Kendala fisik dalam program larasita seperti kendala pada kendaraan, menyebabkan penguluran waktu
	A8	T3	Kerusakan pada jaringan
6	A2	T3	Kerusakan data yang di akibatkan oleh kecelakaan pengguna data(*Accident*)
	A4	T4	Audit sistem yang tidak terlaksana dengan baik menyebabkan terbukanya celah kelemahan sistem
	A6	T1	Penyalah gunaan hak karena tidak adanya sistem keamanan akun
	A6	T3	Tampilan user interface pada software rumit memiliki banyak kesempatan mempersulit proses data
	A9	T2	Jeleknya prosedur rekrutment menyebabkan pegawai kurang terlatih dan memiliki kesempatan menyebabkan kerusakan data
7	A4	T2	*Rogue User* ambisi personal dating dari operator sistem yang dapat menembus sistem dengan melakukan DoS, dan penyalah gunaan hak
	A5	T1	Kesalahan dalam instalasi media penyimpanan terganggunya operasi sistem
	A6	T4	Tidak adanya sistem pengenal user sehingga menyebabkan exploitasi sistem
8	A4	T5	Kelemahan kebijakan tentang aturan penggunaan database data dan user
	A6	T2	Tidak terkontrol alokasi data akun user/operator sistem
	A6	T5	Kerusakan sistem karena software sistem yang belum stabil
	A8	T2	Jaringan komunikasi yang tidak di lindungi, menyebabkan intersepsi data (penyadapan)
	A8	T7	*Denial of Action*
	A9	T1	Ketidak hadiran pegawai menyebabkan ketersediaan data sulit (*availability*)
	A9	T3	Kurang baiknya pelatihan operator sehingga kesadaran akan keamanan sistem tidak di aplikasikan
9	A2	T1	Data digital rawan di modifikasi
		T2	Eror dalam penggunaan sistem sehingga data rawan rusak atau hilang
	A5	T2	Konfigurasi hardware kurang baik
		T3	Kehilangan daya listrik, berhentinya sistem online
	A8	T5	Remote spying karena kelemahan pada arsitektur jaringan
	A9	T5	Pencurian data karena kurangnya monitoring pada sistem
10	A1	T3	Duplikasi data karena salah penempatan data
	A4	T1	Bekas pengguna sistem priviledgenya belum di cabut menyebabkan *Abuse of Right*
	A5	T4	Pencurian data karena proteksimedia penyimpanan tidak ada
	A6	T6	Manajemen password buruk
	A8	T6	Penyebaran password

11	A7	T1	Kerusakan lingkungan sistem, sehingga secara tidak langsung data tidak terjaga
		T2	Rawan bencana alam memiliki kemungkinan kecil
	A8	T1	*Denial of Action* pada kebijakan TI
		T4	*Forging of right* pada data
12	A9	T6	Tidak terkontrolnya akses pegawai pada sistem
		T7	Jeleknya kebijakan tentang penggunaan media informasi
	A10	T1	Tidak teraturnya registrasi user yang baru
		T2	Kebijakan supervisi yang jelek
		T3	Audit yang tidak terlaksana dengan baik pada sistem
		T4	Keterlanjutan perawatan sistem tidak terjaga
		T5	Tidak adanya kebijakan penggunaan email
		T6	Pencurian data karena kebijakan data tentang monitoring tidak terjaga

V. KESIMPULAN DAN SARAN

A. Kesimpulan

a. Penelitian ini dapat memenuhi tujuan awal sehingga di dapatkannya hasil akhir dari proses *Assessment* sampai pada tahap evaluasi resiko.
b. Resiko yang telah teridentifikasi telah di prioritaskan berdasarkan penilaian yang di tentukan menurut standar ISO dari prioritas resiko mana yang paling berpengaruh ke tingkat resiko yang paling kecil.

Data tersebut di butuhkan apabila pada penelitian selanjutnya akan di kembangkan ke beberapa tahap selanjutnya dalam proses *Information Security Risk Management* seperti *Risk Acceptance*, *Risk Treatment* atau keseluruhan tahap sehingga metode model *Plan-Do-Check-Act* dapat di gunakan.

B. Saran

Untuk proses *Context Establishment* dapat di lakukan iterasi atau identifikasi dengan berulang sehingga di dapatkan hasil yang lebih detail jika ingin di kembangkan dengan hasil output yang *Quantitative,* dan kriteria *Assessment* yang lebih detail.

DAFTAR PUSTAKA

BS ISO/IEC . (2008). *Information technology - Security techniques - Information security risk management* (1st ed.). British: British Standards Policy and Strategy Commitee.

Calder, A. (2009). *Implementing Information Security based on ISO 27001/ISO 27002 - A Management Guide.* Zaltbommel : Van Haren Publishing.

ISO/IEC. (2002). *Guide 73, Risk management - Vocabulary - Guidelines for use in standards.*

ISO/IEC. (2006). *16085, Systems and software engineering - Life Cycle processes risk management.*

Kementrian Komunikasi dan Informatika RI. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik.* Kominfo.

Rahardjo, B. (2005). *Keamanan Sistem Informasi Berbasis Internet.*

Rizqi. (2009). *mengenal-istilah-cia-dalam-suatu-sistem.* Retrieved from rizqikautsar.com: http://www.rizqikautsar.com/2013/09/mengenal-istilah-cia-dalam-suatu-sistem.html

Sarno, R. (2009). *Audit Sistem dan Teknologi Informasi.* Bandung: Itspress.

Website Resmi BPN, 2015. www.bpn.go.id